INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 9, Issue 7, (2019) E-ISSN: 2222-6990

Ransomware a Concealed Weapon of Cyber Extortion: The Beginning Unfolded

Haitham Hilal Al Hajri[1], Badar Mohammed Al Mughairi[2], Prof. Dr. Asif Mahbub Karim[3], Md. Nasiruzzaman[4], Mohammad Imtiaz Hossain[5]

[1&2] PhD Researcher, Binary University of Management & Entrepreneurship, Malaysia [3] Dean, Binary Graduate School, Binary University of Management & Entrepreneurship, Malaysia,[4] MSc in ITM, Binary University of Management & Entrepreneuship, [5]MSc in Business Economics,University Putra Malaysia,Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v9-i7/6190 DOI:10.6007/IJARBSS/v9-i7/6190

Published Date: 26 July 2019

Abstract

The technology has indeed resolved so fast, that what it used to be a Sci-Fi movies in yester years, is a conventional reality today. Lot of ordinary accessories' have turned to be smart, especially now we are at the peak of an era of wearable technology and internet of things (IoT). The ongoing growth of innovation within the information and communication technology (ICT) sector is massive, practically the smart mobiles revolution which has shown a large scale adoption that it became an essential part of the daily human interactions. However, cybercriminals have found new grounds to explore potential abuse and misuse, where they have merged and resurrected legacy threats to be implemented on modern tech. This article is methodically illustrating a specific kind of cyber threat known as a ransomware which not only attacks cooperate computers and networks, but it has set the path to newer technology trends such as IoT and smart mobile devices. This paper will also highlight the evaluation of the malware known as ransomware and how it has become a global threat, Additionally to recommend on how to stay protected against such threat.

Keywords: Ransomware, Malware, Cyber Threat, Crypto, Cyber Extortion

Introduction

Ransomware is considered to be among the top consistent and renewable persistent threat in the digital era of technology. However, this threat is not relatively new wave in cybercrimes. Instead, it took a while to be thoroughly be used by cybercriminals until it has become a reality. A digital nightmare that not only hunts the cooperate computers and networks, but it instituted its way to the mobile and internet of things technology. Let us define ransomware to its most basic understanding form and which type of malware code that once it finds a host (target device with open vulnerability). It will actively encrypt all the device content along with associated sub storages (external memory drives /cards) and then display a lock screen

with very demanding ransom (payoff,). U sually done using a cryptocurrency (bitcoin), in order to unlock the encryption and have access to the devices once again.
So in its very simple way, it takes the victim device as a hostage until the ransom is paid, on a timely matter or it the victim will risk losing the encryption keys forever, of course having a time farm is to practice pressure on the victim to pay the ransom transitorily. Let us be clear that this kind of malicious code is designed purely for financial gain purposes, therefore, malware creators aim to infect as many devices as possible, that are linked to ongoing live production environments, ultimately attacker's prime targets are critical infrastructure systems and environments. Such as (transportation, energy sector, healthcare, media, financial sector and military sector). The reason why attackers target the critical infrastructure is due to its critical nature and dependency in various life-threatening situations. Therefore victims' may be under pressure to pay the ransom to gain control of their systems.

Literature Review

According to Palo Alto Networks, Unit 42 report on Ransomware tiled "Ransomware: unlocking the lucrative criminal business model" (Labs, 2016). The first recorded incident of the malicious code ransomware was called the AIDS Trojan AKA (PC Cyborg) created by Dr. Joseph L. Popp, a biologist who had a devoted interest in aids medical research. Where he has distributed 20,000 floppy disk to delegates of fellow aids researchers, containing a malware that activates after 90 reboots, then displays a message instructing to pay a licenses fee of US$ 189 to an account post office box in Panama[1]. The tactic applied and the way it has been executed was considered unconventional for its time. Some might argue it was an evil genius plan if the intention was right. However even when Dr. Joseph was apprehended, prosecutors have had a tough time dealing with the case, as there were no laws introduced to combat such crimes related to technology at that time. Creating such malware as a first of its kind, and from someone who is from a biology background, the malware was coincided as weak, and flow was swiftly discovered. That enabled researchers to reverse the code and find a solution to unlock the encryption and retrieve data and gain access to the device.

Figure 1: Illustration of screen lock of malware Aids *(Networks, 2017)*

Malware Resurrection after 16 years

16 years later specifically in the year of 1996, two enthusiastic researchers Adam Young and Moti Yung have managed to further advance the AIDS malware code, by utilizing public key cryptography to enhance and improve the code encryption, constructing a firm malware that

is considered hard to crack, and consequently it has become more effective in encrypting the targeted device content. The researches have detailed the proof on concept method in their paper titled: Cryptovirology: Extortion-Based Security Threats and Countermeasures (Micro, 2016). Which not only set a new ground to be explored by cyber criminals but it has conclusively demonstrated the power of encryption as an offensive tool that can use on cyber-attacks, rather than the cowman usage of cryptography (encryption) as defensive measure or technique to protect data and information from authorized access.

Ransomware Expansion

From this point forward, cybercriminals and malware code developers have seen the potential abuse of encryption, when its strategically placed on devices that carry a great deal of essential data cybercriminals have found a new grounds to explore and even more creative and luring techniques to be implemented to order to spread the malware code. The period of 2013-2015, several versions of the ransomware virus started to surface that have divers tweaks and upgrades until late 2015 where the cyber world undertook a significant shift towards deploying and distribution of the ransomware malware in a more substantial scale attack. Multiples factors came to play in ministering the disposition of the ransomware virus, starting with the increased manufacture and use of internet-based devices known as the internet of things. Also, the dependency of the population on smart cell phones, have intrigued cybercriminals to think border, that empowered them to create cross-platform malware, to spread malware infection at a larger scale.

The year of 2014, marks the first appearance of mobile-based ransom malware known as the police ransomware and it had variants of Android/Koler or Android/Locker (Micro, 2016). The years 2016-2018 symbols the global infection period, where ransomware malware have had a huge media boost and took headlines by storm due to it fast revolving global infection, which has caused many organization significant financial , data and reputation loss.. Many ransomware malware has become a household name such as WannaCry, Petya, NotPetya, due to its vicious and fast infection globally.

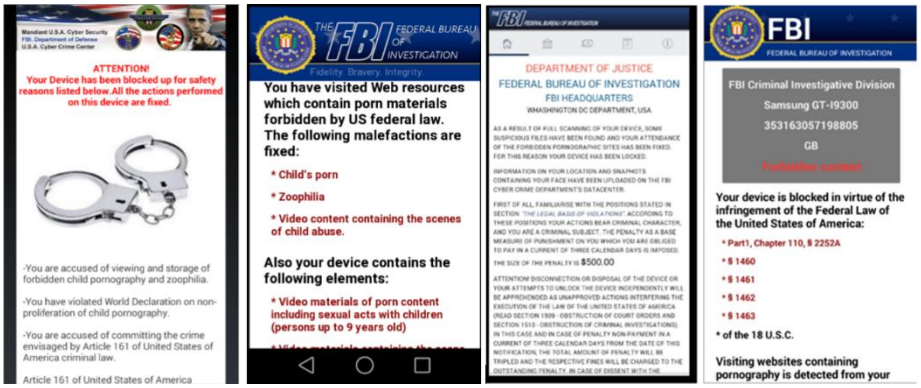

Figure 2:Android Ransom FBI *(Robert Lipovský,Lukáš Štefanko, and Gabriel Braniša, 2016)*

Ransomware Method of Infection

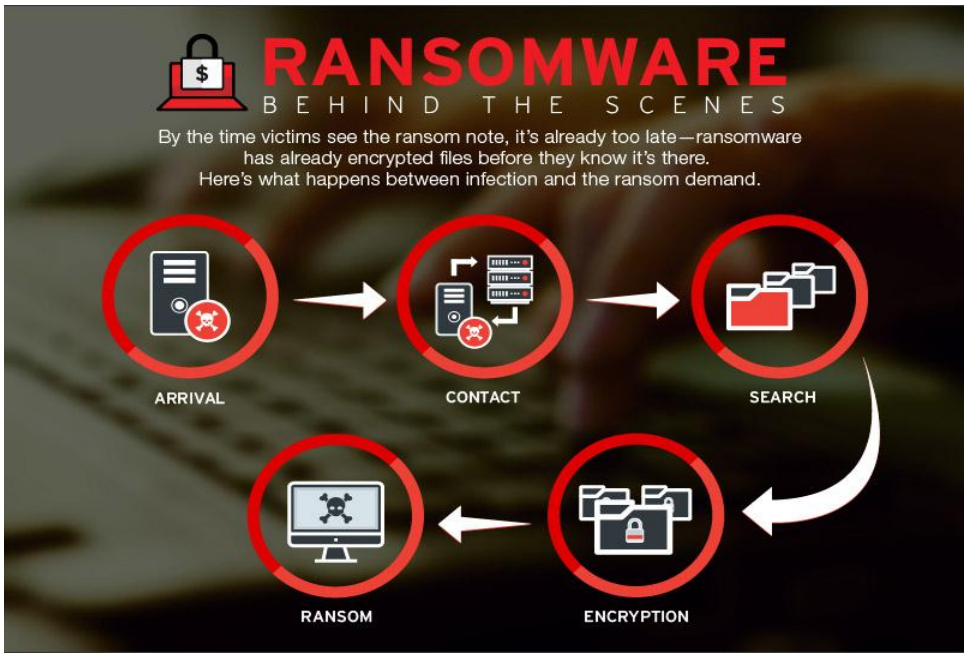

Figure 3: Ransomware Infection Strategy *(Micro, 2016)*

According to Trend Micro article titled Ransomware: Behind the Scenes (2016), the ransomware infection can be demonstrated into five-stage process Figure [3]

Stage 1: ***Arrival***, in this stage the victim or the target receives the malware by activating an infected URL or activating a program that has the malware-code within, cybercriminals are being innovative in conceiving smart methods to lure the victim into enabling and downloading the malware in their system.

Stage 2: ***Contact***, once the malware occupied the host (device), it starts to establish communication with its web server or Command & Control (C&C), begin to exchange information about the host and awaits instruction on when to start encryption and display the ransom message.

Stage 3: ***Search***, at this stage, the malware starts to look for a specific folder or its generally go specific pre-defined folders, it depends on the malware type and configuration by design, some may only be interested in particular files or folders take hostage by encrypting and denying access to it.

Stage 4: ***Encryption***, in this stage the malware starts to generate and deploy the selected encryption algorithm keys, the encryption algorithm chosen may vary depends on the type of system or file is intended for, and some malware utilizes designated or a specific type of encryption that best suits the host.

Stage 5: Ransom, the final step is to display the demanded ransom and instruction on how to deliver the payments to the attacker. The page usually presents time counter to cause panic and rush the victim into making the ransom payment or the encryption key will be destroyed, and the victim will no longer be able to retrieve any of the encrypted materials.

Best Practices and Recommendations

Ransomware threats and attacks have been developing rapidly, and the more cutting-edge code is industrialized by cybercriminals to overcome any security measure in place. Therefore the need to adopt a framework or a security concept to combat against such a threat has become a necessity, many leading cyber security experts and services providers have developed plans and strategies, to aid on reducing the ransom risk of infection. Within this paper will illustrate some of the best practices to deploy against ransomware.

Best Practices to Protect Against Ransomware

Ransomware threats and attacks have been developing rapidly, and the more cutting-edge code is industrialized by cybercriminals to overcome any security measure in place. MacAfee who considered as one of the leading cybersecurity solution software developer and the provider has released an infographic conveying seven best practices in securing against ransomware threat (Lipovský, 2016).

Figure 4: MacAfee Ransomware Best Practices *(Labs, 2016)*

Method 1: ***Device Protection***, in this method to ensure that all devices within any given environment personal or cooperate protected by anti-malware software that is frequently updated and patched.

Method 2: ***Secure communication***, by implementing internal network filters that filter out the malicious traffic and ensures only legit traffic gets to travel to its distention within the network.

Method 3: ***Keep Software Current***, this method to ensure that all software within the system has been updated and patched to the latest edition, to avoid any known holes to be utilized by the malware.

Method 4: ***Sandboxing*** deploying sandboxing within cooperate network will ensure testing of patches or software before it goes to the real environment to avoid any malicious activity.

Method 5: ***Backup Data***, this is the most crucial part is to ensure that frequent backup has been taken and stored in a secure offline location, which can be accessed and retrieved when needed urgently.

Method 6: ***Educate users,*** human factor remains the weakest link within the chain of security. Therefore, conducting regular cyber security awareness will enhance security culture and aid on risk avoidances.

Method 6: ***Access restriction,*** restricting user access will aid in avoiding installation of infected malware within the system, as many of them require admin access to e installed.

Conclusion

Firstly, the paper is based upon various research and published articles, in the area of cybersecurity, specifically within the malware domain, as the dependency on technology is growing rapidly. Cybercriminals will explore other domains to lavage technology to their well, and carry on their deeds, by extorting money or blackmailing their victims. Secondly, ransomware malware has indeed made its mark within the cybercriminal world, as an effective weapon of choice under cyber criminal's arsenal kit. What feuds the spread of such an attack is the enormous adaptation and evolvements of IOT based technology, and the availability of internet connection around the clock in many capacities enables a global outreach of the malware within hours. Finally, since this kind of malware aims to extort money from victims, the availability of anonyms secure payments such as cryptocurrency, make it easy for cybercriminals to get paid without a trace.

There will always be a flow or vulnerability discovered by cybercriminals, best to mitigate against is to deploy most recent best practices and protection frameworks and to have a secondary offline backup that frequently maintained and updated adequately. Finally to ensure that the human factor is aware and ready when such an attack outbreaks, proper incident plan in place to enhance the chances of immediate business recovery.

Corresponding Author
Mohammad Imtiaz Hossain
MSc Scholar, University Putra Malaysia
Serdang, Selangor, Malaysia.
Email: imtiazhossain677@gmail.com

References

Labs, M. (2016). *Taking Steps to Fight Back against Ransomware, McAfee Labs on.* Retrieved from Mcafee Securing Tomorrow: https://securingtomorrow.mcafee.com/mcafee-labs/taking-steps-to-fight-back-against-ransomware/

Micro, T. (2016). *Ransomware: Behind the Scenes .* Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-behind-the-scenes

Networks, P. A. (2017). *Unit 42 Report Ransomware: unlocking the lucrative criminal business model.* Retrieved from paloaltonetworks: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report

Lipovský, P., Štefanko, L., and Braniša, G. (2016). *Rise of Android Ransomware.* Retrieved from welivesecurity: https://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf